A Formal Property Verification for Aspect-Oriented Programs in Software Development

Moustapha Bande, Hakima Ould-Slimane, Hanifa Boucheneb

Abstract—Software development for complex systems requires efficient and automatic tools that can be used to verify the satisfiability of some critical properties such as security ones. With the emergence of Aspect-Oriented Programming (AOP), considerable work has been done in order to better modularize the separation of concerns in the software design and implementation. The goal is to prevent the cross-cutting concerns to be scattered across the multiple modules of the program and tangled with other modules. One of the key challenges in the aspect-oriented programs is to be sure that all the pieces put together at the weaving time ensure the satisfiability of the overall system requirements.

Our paper focuses on this problem and proposes a formal property verification approach for a given property from the woven program. The approach is based on the control flow graph (CFG) of the woven program, and the use of a satisfiability modulo theories (SMT) solver to check whether each property (represented par one aspect) is satisfied or not once the weaving is done.

Keywords—Aspect-oriented programming, control flow graph, satisfiability modulo theories, property verification.

I. INTRODUCTION

WITH THE increasing size and complexity of software systems, most of software development teams need tools or techniques that may help them to detect errors or to find inconsistencies in the source code. Among the various functionality of a program, security modules are more critical because their violation may lead to enormous loss for enterprises. In AOP, it is not accurate to assume that the successful testing in isolation of the base program and each aspect implies the consistency of the overall system, since interactions and interference usually happen between them and changes in one aspect may have significant impacts on the whole execution of the AOP program.

The problem of detecting errors or inconsistencies during the weaving time has been variously tackled by aspect-oriented community. Some of the previous work have focused on...
finding approaches and tools for aspect-oriented program testing, using Unified Modeling Language (UML) models [20], [3], [2] or graph-based testing [12], [25], [5]. In this work, we present another approach that combines some of the existing approaches for verifying the satisfiability of properties covered in a woven aspect-oriented program. Every time, one critical aspect related to a specific property is added to the program, it may be possible to check if all the properties being covered by the program remain satisfied. Indeed, such critical requirements need to be handled with accuracy and only an automatic tool that can explore all the necessary states of the program execution could help to avoid the software misbehavior.

The main contribution of this paper is an automatic misbehavior detection of a given property at the weaving time. It is an integrated approach that uses the control flow graph (CFG) of the woven program and then, by transforming the derived CFG into Z3-SMT solver model, we can easily verify the satisfiability of any property. This work can be extended to any new added aspect and also used in collaborative software development in order to automatically verify whether the woven program still satisfies a given property.

The remainder of this paper is organized as follows. In Section II, we present our formal property verification approach for aspect-oriented programs. Section III deals with our model simulation results and Section IV is dedicated to some previous work in AOP software testing. Section V finally concludes the paper and gives some future work.

II. Formal Property Verification in AOP Programs

For our design purpose, we use an automatic teller machine (ATM) transaction management system.

A. Experimental Example: An ATM Transaction Management

As we can see, this example refers to an ATM transaction management in an AspectJ program.

The listing 1 shows the Java class BankAccount which simulates the functionality of a bank account and represents the base program. The aspect defined in Listing 2 is used to monitor the access to a bank account by a user. This aspect captures the authentication access control. We define another aspect in Listing 3 that captures transaction checking (e.g. being sure that an account has enough money for a withdrawal transaction). Our experimental source code example consists of one class (BankAccount) and two aspects (authentication and transaction checking).

- **Class BankAccount.** This class records user’s account information: user name, account ID, pin code and account balance. It also defines methods such as withdrawal and deposit.

- **Aspect AspectAuthentication.** This aspect implements authentication goal. That is giving access to authorized users to their account information. The goal that keeps the information secret from unauthorized people is almost the most common one in information security. In the context of ATM transaction management, violation of such an information security property may be crucial for the bank reputation.

- **Aspect AspectChecking.** It implements a transaction requirement checking. We use a before advice to check whether a withdrawal transaction is possible or not considering the target account balance. It also includes a after advice that simply displays the target account balance after the transaction has been successfully completed.

Given an aspect-oriented program and any property that may be verified through the execution of this program, we build a fully integrated approach that verifies if the property is satisfied or not during the weaving time.

B. Our Design Approach

Our framework in Fig. 1 uses an existing algorithm that aims to generate the control flow graph of the program and a formal system verification tool that is used to verify the SMT solver from the generated CFG and also to verify that some properties can be automatically verified.

For our design purpose, we use the algorithm proposed by [21] to generate the CFG of our program. In their work, the authors implemented a tool called AjCfGraphBuilder that automatically derives an aspect-oriented control flow graph (AOCFG) giving an AOP program. Based on their algorithm, Fig. 2 shows the CFG of our AOP program and displays the information necessary with the character $B$ followed by the line number of the source code for the Base program and $A$ by the line number of the source code for the AspectAuthentication program and $C$ for AspectChecking program. The small $b$ added to the node $B78b$ and $B79b$ stands for before advice, whereas small $a$ added to node $B79a$ is used for after advice. We also add (in yellow color) nodes and edges that denote the case where the pin code is not valid $(A8 \Rightarrow A11 \Rightarrow A12)$ and the one where account balance is less than the withdrawal amount $(C7 \Rightarrow C8 \Rightarrow C9)$.
```java
package example;
import example.BankAccount;
import java.io.*;
import java.util.Properties;

public class BankAccount {
    private String accountOwner;
    private String accountNumber;
    private String accountPin;
    private double balance;

    public BankAccount(String owner, String account, String pin, double balance) // BankAccount constructor
    {
        this.accountOwner = owner;
        this.accountNumber = account;
        this.accountPin = pin;
        if (balance > 0.0)
            this.balance = balance;
    }

    public void deposit(double depositAmount) // method for deposits
    {
        balance = balance + depositAmount; // update the balance
    }

    public void withdrawal(double withdrawalAmount) // method withdrawal
    {
        balance = balance - withdrawalAmount; // update the balance
    }

    public double getBalance()
    {
        return balance;
    }

    public void setAccount(String account)
    {
        this.accountNumber = account;
    }

    public void setOwner(String owner)
    {
        this.accountOwner = owner;
    }

    public void setPin(String pin)
    {
        this.accountPin = pin;
    }

    public String getOwner()
    {
        return accountOwner;
    }

    public String getAccount()
    {
        return accountNumber;
    }

    public String getPin()
    {
        return accountPin;
    }

    public boolean authenticate(String userName, String pin) throws Exception
    {
        File userFile = new File("D:/eclipse/workspace/users.txt");
        FileInputStream in = new FileInputStream(userFile);
        Properties properties = new Properties();
        properties.load(in);
        String storedPassword = properties.getProperty(userName);
        in.close();
        return pin.equals(storedPassword);
    }

    public static void main(String[] args)
    {
        BankAccount account = new BankAccount("Toto","120541263","789",500);
        account.deposit(500);
        account.withdrawal(300);
    }
}
```
Fig. 2 The derived CFG of our program

Listing 2: Aspect user’s authentication

```java
package org.example.aop;
import example.BankAccount;
public aspect AspectAuthentication {
    pointcut authentication (BankAccount b, double x): (call(* BankAccount.withdrawal(..)) || call(* BankAccount.deposit(..))) && target(b) && args(x);

    before(BankAccount b, double x) : authentication(b, x) {
        try {
            if (!b.authenticate(b.getOwner(), b.getPin())) {
                System.out.println("Access denied ... Incorrect pin");
                System.exit(0);
            }
        } catch (Exception e) {
            System.out.println("Error ...");
        }
    }
}
```

Listing 3: Aspect transaction checking

```java
package org.example.aop;
import example.BankAccount;
public aspect AspectChecking {
    pointcut checking(BankAccount b, double x): call(* BankAccount.withdrawal(..)) && target(b) && args(x);

    before(BankAccount b, double x) : checking(b, x) {
        if (b.getBalance() < x) {
            System.out.println("Sorry Your account does not have. \$" + x + " to withdrawn...");
            System.exit(0);
        }
    }

    after(BankAccount b, double x) : checking(b, x) {
        System.out.println("Transaction successfully done !!! Your current balance is : \$" + b.getBalance());
    }
}
```
After the generation of the CFG graph, we build our model by deriving Z3 SMT model from the CFG graph.

C. Our Z3 Model Design

Satisfiability Modulo Theories (SMT) is the Satisfiability of formulas with respect to some background theory [4]. According to the authors in [8], Z3 is a new SMT solver tool from Microsoft Research. This tool aims at checking the satisfiability of logical formulas over one or more theories and is based on first-order logic. A given formula $\phi$ is said to be satisfiable if there exists an interpretation that makes $\phi$ true. A formula is said to be valid if it is true under all structures. For example, $x + y > 3$ is satisfiable under the interpretation $x \mapsto 1$ and $y \mapsto 3$. We report in this paper only some relevant Z3 constructs that we use in our model due to the limit of the paper length. For our model design purpose, we use Z3Py, a Python interface for Z3 solver.

- **Sorts.** Z3 allows users to declare new data types called sorts (e.g. $a = \text{DeclSort}(\text{"a"})$).
- **Constants.** They are functions that take no argument (e.g. $b = \text{Cons}(\text{"b"}, a)$).
- **Quantifiers.** Universal quantifier is represented by $\forall x$. Existential quantifier is represented by $\exists x$. For all and existential one by $\text{Exists}$. We recall that the goal of our model is to automatically verify properties for an AOP program. Based on the parameters used to run the main method, we verify whether an unauthorized user could access or not the ATM system. After building our Z3 model, we add some constraints into it and then check its satisfiability.

First of all, we add the constraint

$$s.\text{add}(\forall [u_i, p_i]. \text{Implies}(\text{Not}(\text{isAuth}(u_i, p_i)), \text{g.es}[11][\text{"ExecStatus"}]))$$

(1)

The checking of the solver using $\text{print}(s.\text{check}())$ outputs the result $\text{Sat}$ meaning that our model is satisfiable. This shows that for any given user $u_i$ and his pin code $p_i$, if the pin code is not valid then we do have an edge between nodes $A11$ and $A12$. The attribute $\text{ExecStatus}$ of this edge is then True corresponding to the edge whose index is $11$. Consequently, the access is denied and the end node is $A12$. We output only the part of the graph with edges having their execution status at true in Fig. 3.

We also add to the solver this constraint

$$s.\text{add}(\forall [u_i, p_i, b_i, x]. \text{Implies}(\text{And}(\text{isAuth}(p_i, f_i), x <= b_i), \text{g.es}[32][\text{"ExecStatus"}]))$$

(2)

Then, we run the model using $\text{check}()$ method and the output result of the model checking is $\text{Sat}$, that is the user $u_i$ has entered a valid code pin and the withdrawal amount is less than his account balance, so that the transaction is successfully completed. Thus, the attribute $\text{ExecStatus}$ of the edge whose index is $32$ is True. Consequently, the end node in the output in Fig. 4 is $C14$.

Finally, We add to the solver the following constraint that verifies whether the user do not enough money to make his withdrawal transaction.

$$s.\text{add}(\forall [u_i, p_i, b_i, x]. \text{Implies}(\text{And}(\text{isAuth}(p_i, f_i), x > b_i), \text{g.es}[27][\text{"ExecStatus"}]))$$

(3)

Then, we run the model using $\text{check}()$ method and the output result of the model checking is $\text{Sat}$, that is, the user has access to the ATM system but his account balance is not enough to make his withdrawal transaction. Thus, the
attribute "ExecStatus" of the edge whose index is 27 is True. Consequently, the end node in the output in Fig. 5 is C9.

We note that the increase of the number of users does not affect the size of our model since the system follows the execution of the main() method. In addition, it is also possible to define other types of properties and add them to the model and let Z3-SMT solver checks the satisfiability of the whole system. In Z3, it is possible to handle function composition, that is a function call in the CFG that also calls other functions. We could also add this kind of constraint to the model and check the solver satisfiability. That helps to make modular verification and also incremental one. Our model is flexible and could be used whenever a developer adds a new aspect that captures a specific concern. It can be extended to a collaborative environment where developers together add components in a base program.

### IV. RELATED WORK

Many researches have focused on software testing using several formal methods and tools to detect faults and errors during compilation or running time. These approaches can be classified into three categories:

The first category is related to those approaches that use model checking to verify whether a given property is verified or not. Among them, in [13], the authors proposed an aspect-oriented Petri net with Aspect-Oriented Software Development (AOSD) mechanisms. They developed an automated approach for formally analyzing the software design using the model checking technique and analysis tool PROD. In [27], Xu et al. presented a framework called Model-based Aspect/class Checking and Testing (MACT) that aims to test the conformance of aspect-oriented programs against their aspect-oriented state model. The framework also uses model checking for test generation from counterexamples. Fradet et al. [11] proposed a formal framework to enforce availability properties on services sharing resources. The authors used timed automata in order to express and enforce properties on execution time. In [24], they defined an automatic verification approach using model checking that verifies the correctness of AOP-based programs. In order to check the correctness of the woven program, they defined a...
property in Computation Tree Logic (CTL) and represent this property by an aspect that is finally used for the property verification. In [9], Denaro et al. proposed an approach based on analyzing aspect-based software components in order to verify safety properties. The aspects are modeled using a PROMELA process template and the derived model is analyzed with the model checker SPIN in order to verify the deadlock problem of the synchronization policy. Another state-based approach has been proposed in [26] for modeling the specification of an aspect-oriented design. In this paper, the authors used a Labeled Transition System Analyzer (lTSA) model checker to verify the generated finite state processes against the desired properties. In [22], a runtime verification framework for Java programs has been proposed. They instrumented Java bytecode with Linear-time Temporal Logic (LTL) formula and for the properties verification purpose, they used an automaton-based approach where transitions are implemented and triggered using aspects. They also developed a prototype called Java Logical Observer (JLO) that gives a way to derive a verification aspect from the formula. The technique used in this paper, however, implies injecting aspects in order to verify a specific property. That can become more challenging while the number of properties being verified grows. These papers did not, however, describe a modular verification methodology or most of them use source code instrumentation for the verification purposes.

The second category of related work is data-flow or control-flow based testing approaches. In [18], a pointcut-based coverage analysis approach using structural model based on Java bytecode has been proposed. In their approach, the authors used a control and data flow graph for their testing criteria. They also proposed a series of control flow and data flow testing criteria based on a PointCut-based Def-Use (PCDU) graph. However, they did not mention the data flow between integrated units among their testing criteria. In [28], the author proposed a data-flow-based unit testing approach in which three levels of testing are performed: intra-module, inter-module and inter-aspect or inter-class testing. The model is based on modeling a control graph flow for only the program classes and is extended to the woven program. Finally, the program issues are analyzed by computing def-use pairs of a class or an aspect. This work, however, does not focus on the advice interactions. Fradet et al. [11] proposed a formal framework to enforce availability properties on services sharing resources. The authors used timed automata in order to express and enforce properties on execution time for preventing denial of service attacks. However, they did not consider any change that may occur in the source code. In [19], a derivation of control flow and data flow based testing criteria for aspect-oriented programs has been defined. This model is used to support structural testing to unit testing of AspectsJ programs. The key problem with existing dataflow test criteria is the difficulty in covering all types of data flow interactions for AOP programs. Harlem et al. [14] proposed an aspect-oriented declarative security policy specification language for in-lined reference monitoring. This language called SPOX (Security Policy XML) is an XML-based security policy specification in which policies denote an aspect-oriented security automaton.

In the first category of the aforementioned work, the authors instrumented the source code by injecting pieces of code (e.g. aspects) in order to verify a specific property. In the second category, testing criteria are defined on control flow without taking into account the data flow or the core program and the aspects are tested separately. Unlike the above work, our paper focuses on verifying a security property (e.g. authentication, privacy, etc.) encapsulated in an aspect for a woven program and also captures the interactions between the base program and the aspects.

The third category is UML-based transformation using sequence diagrams. Hossain et al. [15] proposed a transformation technique called “Zigzag transformation” to introduce aspects at the architecture level in order to verify properties of the old architecture versus the ones introduced by the aspects. Bowles et al. [6] introduced a novel formal automated technique for weaving aspects using Z3-SMT solver. Their technique is based on UML sequence diagrams to capture the base and the advice and pointcut models are transformed into equivalent representations using Labelled Event Structures (LES). They also compared the performance using Z3 with their earlier work that used Alloy [6] for sequence diagram composition. Tahara et al. [23] proposed a tool called "CAMPer" that uses Maude specification language to express dynamic aspect weaving. This tool takes an input UML class diagram, sequence diagrams and a Linear Temporal Logic (LTL) formula and automatically verifies the models.

Unlike the aforementioned work, our approach combines control flow graph generation and a SMT solver to check the satisfiability of properties by deriving a Z3 SMT model from the CFG.

V. CONCLUSION AND FUTURE WORK

In this paper, a formal verification of properties in aspect-oriented programming is proposed. The main idea of our approach is to generate a control flow graph from a given woven aspect-oriented program and to derive Z3-SMT model in order to verify some critical properties such as confidentiality. Our approach is flexible and can be extended to both AOP programs with many aspects that encapsulate security property or specific requirement and collaborative software development environments where many developers can collaborate in the same project. In such an environment, this formal verification technique could be used to verify critical properties whenever any developer adds or modifies a piece of code (e.g. aspects, base program).

As future work, we are planning to extend this work to a collaborative software development including dealing with many aspects. Finally, we will look into building a tool that can automatically generate Z3-SMT model from the CFG.

REFERENCES


